ISMS as a management tool for XAIT

Certifiable ISMS strengthen cyber resilience and contribute to meeting XAIT requirements

Dr. Waldemar Grudzien
Leon Kuhlmann
Moritz Treutwein

August 2022
Blogpost

Public

Key Facts

- A certifiable information security management system (ISMS for short) based on ISO 27001 makes a major contribution to meeting the XAIT requirements[1] (BAIT[2] , KAIT[3] , VAIT[4] , ZAIT[5]) in the regulation of the German financial market.
- XAIT circulars contain sector-specific in-depth information that goes beyond ISO 27001 as well as detailed requirements regarding the design of the ISMS, which must be considered in addition to the standard.
- With the introduction of the EU Digital Operational Resilience Act (DORA for short), an ISMS becomes an EU-wide requirement for affected entities
- Initial indications are that ISMS certification could become mandatory for selected processes with upcoming regulatory cycles

1. Introduction

Studies by the digital association Bitkom show that cyber-attacks in the form of sabotage, data theft or espionage cause high damage: in Germany, this amounted to around 100 billion euros in 2018/2019, before more than doubling to over 200 billion euros in 2020[6]. The data basis for these values is a cross-industry study with managing directors and security managers of German companies. These figures illustrate the importance of an ISMS; after all, the probability of success of such cyber-attacks is drastically minimised using an ISMS. Specifically, this is done by establishing guidelines and implementing the required processes and controls to ensure information security.

In addition, the introduction of a certifiable ISMS is also recommended for organisations from a regulatory point of view: Institutions that are subject to the supervisory requirements for IT of the BaFin (BAIT, ZAIT, KAIT, VAIT; in short: *XAIT*) can fulfil a large part of the regulatory requirements with the help of an ISMS (*see Figure 1*) with the help of an ISMS and provide proof of information security that is accepted on the market by means of a certificate issued by accredited auditors. In addition, the Digital Operational Resilience Act (DORA) will set EU-wide requirements for an ISMS as an EU regulation.

2. Components of an ISMS

Information security management systems consist of numerous internal organisational guidelines, processes and controls that serve the protection of information as well as the structured recording of information risks and suitable mitigation measures.

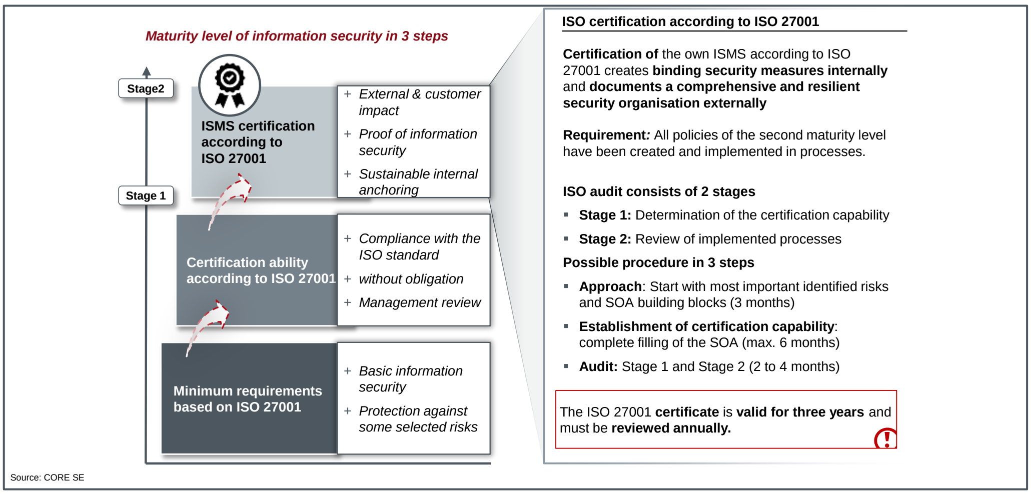
According to BSI[7], a management system comprises all regulations for the goal-oriented control and guidance of an institution. It first defines goals as procedures and rules in guidelines

[1] Word neologism of CORE, summarising the BaFin circulars on requirements for IT (BAIT, KAIT, ZAIT and VAIT)
[2] BAIT: Banking supervisory requirements for IT
[3] KAIT: Capital Management Supervisory Requirements for IT
[4] VAIT: Insurance supervisory requirements for IT
[5] ZAIT: Payment services supervisory requirements for the IT of payment and e-money institutions
[6] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
[7] BSI Standard 200-1: "Information Security Management Systems (ISMS)

("policies"). These provide the framework for the processes to be implemented in practice ("process descriptions" and "work instructions"). ISO 27001 is considered the established standard for setting up and operating an ISMS, supplemented by the implementation instructions and controls of the ISO 27002[8] standard. An ISMS according to ISO 27001 is divided into an overarching High Level Structure (HLS) and 14 basic security objectives (Security Controls A.5 to A.18).

3. Three-step structure of an ISMS

Information security systems can be built up in a structured way over three steps:


Maturity level of information security in 3 steps
Stage2
Stage 1
ISMS certification according to ISO 27001
+ External & customer impact
+ Proof of information security
+ Sustainable internal anchoring
Certification ability according to ISO 27001
+ Compliance with the ISO standard
+ without obligation
+ Management review
Minimum requirements based on ISO 27001
+ Basic information security
+ Protection against some selected risks

ISO certification according to ISO 27001

Certification of the own ISMS according to ISO 27001 creates **binding security measures internally** and **documents a comprehensive and resilient security organisation externally**

Requirement: All policies of the second maturity level have been created and implemented in processes.

ISO audit consists of 2 stages

- **Stage 1:** Determination of the certification capability
- **Stage 2:** Review of implemented processes

Possible procedure in 3 steps

- **Approach**: Start with most important identified risks and SOA building blocks (3 months)
- **Establishment of certification capability**: complete filling of the SOA (max. 6 months)
- **Audit:** Stage 1 and Stage 2 (2 to 4 months)

The ISO 27001 **certificate** is **valid for three years** and must be **reviewed annually.**

Source: CORE SE

Figure 1: Structure of ISO 27001 standard, policy types and aspects of implementation

In the first step, the processes important for certification are checked for relevant risks and addressed by means of protective measures. Important processes are firstly those processes for which the certificate is to apply - the scope of the certificate; and secondly, they are all processes that are necessary for the functioning of the first-mentioned scope processes.

For example, a provider of a video identification procedure will declare this procedure as a process to be certified in the scope of the certificate. Other important sub-processes are needed for the video identification process to function, such as pattern recognition for sovereign ID documents and image recognition for faces.

Based on a risk-oriented approach, corresponding guidelines are first established for the most important subject areas - common examples of this are specifications for risk management, identity, and access management (IAM for short) or also document control, for example with specifications regarding release, communication and publication processes of ISMS-relevant guidelines and processes.

In the second stage, the ISMS is set up holistically in accordance with ISO 27001. The leading document, which is also mandatory for certification, is the Statement of Applicability (SoA), in which the organisation explains the applicability of the individual domains of the ISO standard.

[8] Information technology - Security techniques - Code of practice for information security controls

This statement of applicability is based on Annex A of ISO 27001 - or ISO 27002, which in the current version of 2022 still contains a total of 93 so-called controls.

The following is a brief explanation of the context of these standards:

ISO 27001 is a so-called management standard (as it describes the standard for the operation of an ISMS) and thus also enables certification. Basically, the controls described in Annex A of ISO 27001 can be found with the same name and numbering in ISO 27002 but are described in much more detail there. Currently, however, there is a discrepancy regarding the numbering, as ISO 27002:2022 - unlike the expected update ISO 27001:2022 - has already been published with the following changes:

Compared to the last valid version, the number of controls has decreased from 114 to 93, with 11 new controls added. Many existing controls have been merged and the number of main domains has also been reduced from 14 to 4 and now includes controls for the *Organizational, People, Physical and Technological* domains.

If organisations declare individual measures in their SoA as not applicable, this must be explained with a comprehensible justification - also in preparation for a possible certification. The aim of the applicability declaration is thus also to make any existing deficits regarding guidelines, processes or controls visible in a first step, in order to be able to subsequently create and implement them in a structured manner. The way in which the respective measures are implemented should also be explained in the declaration of applicability, so that the SoA plays a central role in both the development of the ISMS and the eventual certification.

By building up the complete policy volume with the processes and controls included, the certification capability is established. This capability can be proven in the third, optional stage within the framework of an audit, divided into two stages.

4. Information security certification

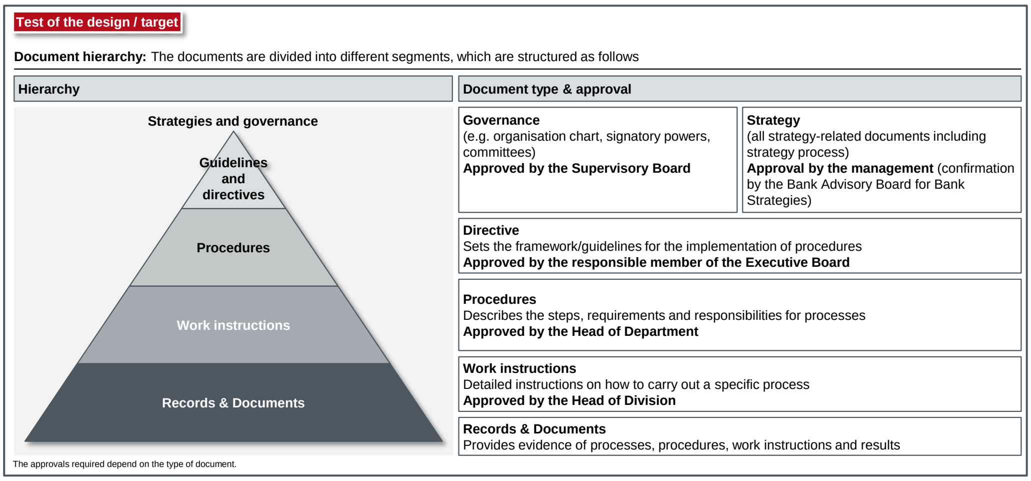
For information security certification according to ISO 27001, it should first be noted that this is only carried out for individual processes and not for an entire company. For this reason, the intended scope of the certification is first determined during the audit.

The stages for initial certification mentioned in advance are structured as follows:

- **Stage 1**: In this stage, the certification ability is confirmed, concrete verification actions include a review of the SoA as well as the policy volume to confirm the so-called "Test of Design" (ToD).
- **Stage 2**: This is followed by the "Test of Effectiveness" (ToE), in which the implementation of the processes and controls according to the SoA are checked.

After a successfully completed audit, an ISO 27001 certificate with a validity of three years is issued for the defined scope. In years two and three, annual reviews take place within the framework of so-called surveillance audits, before a recertification audit becomes necessary at the end of the three years. The programme starts all over again with a major audit of all domains.

Figure 2 shows an overview of the document hierarchy for the complete proof of the "shall" (Test of Design) to be anchored in the sfO (written order, “schriftlich fixierte Ordnung”).



Test of the design / target

Document hierarchy: The documents are divided into different segments, which are structured as follows

Hierarchy	Document type & approval	
Strategies and governance	**Governance** (e.g. organisation chart, signatory powers, committees) **Approved by the Supervisory Board**	**Strategy** (all strategy-related documents including strategy process) **Approval by the management** (confirmation by the Bank Advisory Board for Bank Strategies)
Guidelines and directives	**Directive** Sets the framework/guidelines for the implementation of procedures **Approved by the responsible member of the Executive Board**	
Procedures	**Procedures** Describes the steps, requirements and responsibilities for processes **Approved by the Head of Department**	
Work instructions	**Work instructions** Detailed instructions on how to carry out a specific process **Approved by the Head of Division**	
Records & Documents	**Records & Documents** Provides evidence of processes, procedures, work instructions and results	

The approvals required depend on the type of document.

Figure 2: Example of a document hierarchy for a Test of Design

5. ISMS-relevant regulatory requirements in the financial sector

However, there are no regulatory requirements for the certification of an ISMS - yet. It is therefore not surprising that the number of ISO 27001-certified companies in Germany remains in the low four-digit range. In the financial sector, at least the content requirements for corresponding ISMS are formulated within the framework of the XAIT circulars BAIT (Banking Supervisory Requirements for IT, Preface 3), ZAIT (Payment Services Supervisory Requirements for IT of Payment and Electronic Money Institutions, Preface 3), KAIT (Capital Management Supervisory Requirements for IT, Preface 2) as well as VAIT (Insurance Supervisory Requirements for IT, Preface 6) and thus also represent the basis for supervisory audits. We have already discussed last year's and this year's updates of the ZAIT in comparison to the BAIT[9] and VAIT[10] in previous blog posts.

In the following, the authors refer to individual circulars of BaFin. These circulars were evaluated collectively, merged in XAIT and describe a solution preferred by the authors of a common IT requirements catalogue for banks, capital management companies, payment and e-money institutions as well as insurance companies with sector-specific supplements.

The regulatory classification of these circulars is made in the respective preliminary remarks and is presented below using the BAIT as an example: "This circular provides a flexible and practical framework for the technical and organisational equipment of the institutions - in particular for the management of IT resources, information risk management and information security management - on the basis of § 25a para. 1 of the German Banking Act (KWG)."[11] For the sake of completeness, it should be mentioned here that the legal basis for ZAIT, VAIT and KAIT is provided

[9] https://core.se/de/blog/zait-vergleich-zur-bait
[10] https://core.se/de/blog/vait-aktualisierung-2022
[11] BAIT, 1, No. 2

by the Payment Services Supervision Act (ZAG), the Insurance Supervision Act (VAG) and the Capital Investment Code (KAGB).

Equally relevant is number 3 of the BAIT preliminary remarks, which clarifies that the circulars are to be understood, among other things, as a concretisation of the minimum requirements for risk management (MaRisk), but that their requirements remain fundamentally unaffected. Also worth mentioning is the addition that institutions are still obliged to "(...) generally base the design of the IT systems and the associated IT processes on common standards. These include, for example, the IT-Grundschutz of the Federal Office for Information Security and the international security standards ISO/IEC 270XX of the International Organization for Standardization".

Although institutions are basically free to choose the standards, they must name the standards selected for orientation in the areas of IT and information security in the IT strategy and describe the intended scope of implementation. In addition to the requirement to provide information security management with adequate resources, both quantitatively and qualitatively, the circulars also call for the appointment of information security officers (ISOs), who are ultimately responsible for the information security area.

6. Fulfilment of XAIT requirements with the help of an ISMS

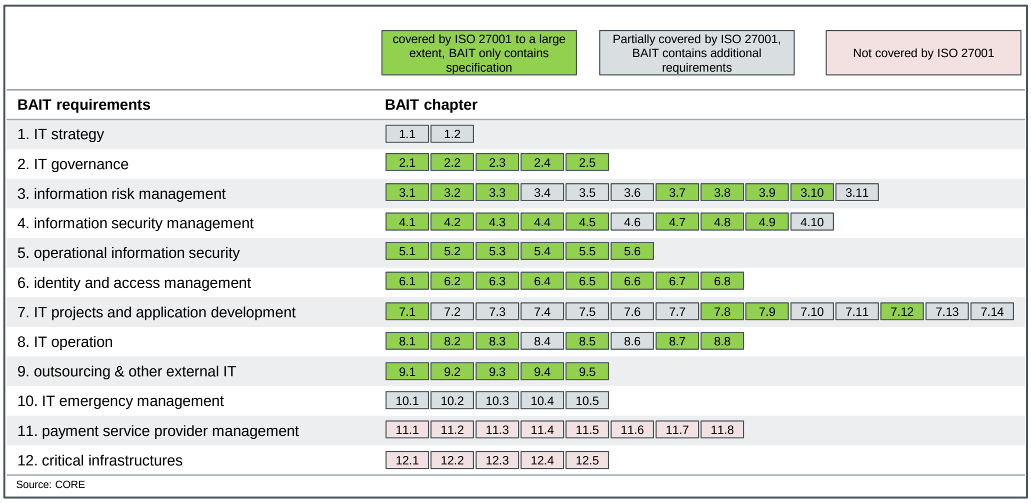
An ISMS plays a central role in meeting XAIT requirements. Earlier, we outlined the structure of an ISMS in three steps: starting with the fulfilment of minimum requirements, then the preparation of the applicability statement with subsequent gap closure and the final, optional certification. For XAIT-regulated organisations, this process model results in an additional step with a gap analysis from ISO 27001 to the respective applicable XAIT circular.

The necessity of the gap analysis arises from the fact that ISO and BSI standards do not contain any sector-specific specifications. Put simply, the standards define a basic setting of the organisation in relation to the domain organisation-technology-human-rights but claim to be equally applicable to all organisations regardless of the business model.

For example, ISO 27001 requires the function of the information security officer. The sector-specific, supervisory circulars subsequently define the required structure with clear, financial sector-specific requirements and specifications for the position of the information security officer. This circular argument from the ISO standard and XAIT results, among other things, from the security objective A.18 (Compliance) of the ISO standard, through which organisations are required to identify legal obligations applicable to them to avoid violations of legal, contractual, statutory or regulatory obligations.

These - in the case of XAIT - sector-specific requirements thus ensure the necessity of a gap analysis. To anticipate the result of such an analysis to some extent: in Figure 3 the authors have illustrated a BAIT-ISO 27001 comparison. It is clear that a large number (marked in green) of the BAIT requirements are to be understood as specifications of existing ISO requirements and not as additional requirements.

The BAIT requirements marked in light red are not included in the ISO standard due to their strongly industry-specific character; specifically, this applies to the topics of *managing relationships with payment service users* and *critical infrastructures (in short: CRITIS)*. The BAIT requirements marked in grey go beyond a pure industry specification. They are partially reflected in this form in the ISO standard and can be understood as additional requirements:



🟩 covered by ISO 27001 to a large extent, BAIT only contains specification

⬜ Partially covered by ISO 27001, BAIT contains additional requirements

🟥 Not covered by ISO 27001

BAIT requirements	BAIT chapter													
1. IT strategy	⬜ 1.1	⬜ 1.2												
2. IT governance	🟩 2.1	🟩 2.2	🟩 2.3	🟩 2.4	🟩 2.5									
3. information risk management	🟩 3.1	🟩 3.2	🟩 3.3	⬜ 3.4	⬜ 3.5	⬜ 3.6	🟩 3.7	🟩 3.8	🟩 3.9	🟩 3.10	⬜ 3.11			
4. information security management	🟩 4.1	🟩 4.2	🟩 4.3	🟩 4.4	🟩 4.5	⬜ 4.6	🟩 4.7	🟩 4.8	🟩 4.9	⬜ 4.10				
5. operational information security	🟩 5.1	🟩 5.2	🟩 5.3	🟩 5.4	🟩 5.5	🟩 5.6								
6. identity and access management	🟩 6.1	🟩 6.2	🟩 6.3	🟩 6.4	🟩 6.5	🟩 6.6	🟩 6.7	🟩 6.8						
7. IT projects and application development	🟩 7.1	⬜ 7.2	⬜ 7.3	⬜ 7.4	⬜ 7.5	⬜ 7.6	⬜ 7.7	🟩 7.8	🟩 7.9	⬜ 7.10	⬜ 7.11	🟩 7.12	⬜ 7.13	⬜ 7.14
8. IT operation	🟩 8.1	🟩 8.2	🟩 8.3	⬜ 8.4	🟩 8.5	⬜ 8.6	🟩 8.7	🟩 8.8						
9. outsourcing & other external IT	🟩 9.1	🟩 9.2	🟩 9.3	🟩 9.4	🟩 9.5									
10. IT emergency management	⬜ 10.1	⬜ 10.2	⬜ 10.3	⬜ 10.4	⬜ 10.5									
11. payment service provider management	🟥 11.1	🟥 11.2	🟥 11.3	🟥 11.4	🟥 11.5	🟥 11.6	🟥 11.7	🟥 11.8						
12. critical infrastructures	🟥 12.1	🟥 12.2	🟥 12.3	🟥 12.4	🟥 12.5									

Source: CORE

Figure 3: Coverage of BAIT requirements in ISO 27001

It becomes clear that a complete implementation of an ISMS based on the ISO 27001 standard directly fulfils numerous BAIT requirements. Within the framework of the gap analysis, there are - briefly summarised - requirements that go beyond this, particularly in the following areas:

- *BAIT Chapter 1 - **IT Strategy***: Not part of ISO 27001 due to the Information Security Scope.
- *BAIT Chapter 3 - **Information Risk Management (IRM)***: Even though a large part of the IRM requirements is found in the ISO standard, there are exceptions for Chapters 3.4 to 3.6, which introduce so-called protection requirements as well as the concept of the information network. According to the ISO standard, companies are required to identify and inventory corresponding assets. However, the ISO standard does not include a requirement for the classification of protection needs and the classification as an information network.
- *BAIT Chapters 3 and 4 - **Information Risk Management (IRM)** and **Information Security Management (ISM)***: Another deviation arises in the subject areas IRM (Chapter 3.11) and ISM (Chapter 4.10) for reporting to the management, which is required at least quarterly in the BAIT
- *BAIT Chapter 4 - **Information Security Management (ISM)***: While the ISO 27001 standard only requires the appointment of an information security officer, the XAIT requirement (BAIT: Chapter 4.6) goes one step further and requires that this position must be held within the institution - outsourcing is thus excluded.
- *BAIT Chapter 7 - **IT projects***: The XAIT formulate numerous requirements for IT projects and application developments, which are not found in the ISO 27001 standard due to the thematic delimitation (BAIT chapters 7.2 to 7.7, 7.10, 7.11). ISO 27001 only

formulates information security-related requirements in this regard, while the XAIT explicitly refer to all IT projects and define general minimum contents for project management.

- *BAIT Chapter 8 - **IT operations***: A large part of the XAIT requirements regarding IT operations can be derived from ISO 27001, exceptions exist regarding functional testing: ISO 27001 only requires the verification of IS-relevant aspects as well as performance failures.
- *BAIT Chapter 10 - **IT emergency management***: In A.17, ISO 27001 formulates measures for information security aspects as part of business continuity management. Explicit requirements on the topic of IT emergency management analogous to XAIT cannot be found in the ISO standard; instead, reference is made to BSI 200-4.

7. EU-wide regulation of an ISMS by DORA

With the Digital Operational Resilience Act, the goal of strengthening cybersecurity and resilience in the financial sector will also be anchored at European level in addition to the EBA Guidelines, after all, the regulation will apply to all EU-regulated financial companies, apply to all EU-regulated financial firms. This additional EU requirement should contribute to a further increased spread of ISMS.

Specifically, in Article 5 (ICT Risk Management Framework), paragraph 4, the regulation requires the Application of a "system for the management of information security" - in other words: an ISMS in its purest form; in a similar form already required by regulation in the XAIT circulars. It remains to be said, however, that such comprehensive ISMSs are far from being established in practice.

And even if DORA, like XAIT, does not yet include a requirement for certification of an ISMS, there are indications that this could change in the next iterations of the regulation in about three to five years - at least for selected processes. For affected institutions, it is therefore obvious to design the development or adaptation of the ISMS with the goal of a corresponding certification.

With accurate implementation, organisations can achieve an ISMS that is both certifiable and meets all XAIT requirements at the same time. A holistic view and implementation of an ISMS is a competitive advantage for financial companies.

Conclusion

The introduction of a certifiable information security management system is currently not mandatory. However, in the XAIT circulars, BaFin formulates requirements for the IT of corresponding organisations. These must understand XAIT as a supplementary industry specification and the ISO 27001 standard as an in-depth requirement. With the help of a certifiable ISMS, a large part of the XAIT requirements can be met directly.

Looking to the future, a certifiable ISMS is desirable for several reasons: on the one hand, steadily increasing numbers of cyber-attacks demand higher cyber resilience from institutions and players in the German financial market, for which an ISMS represents the central management system. On the other hand, the Digital Operational Resilience Act makes an ISMS mandatory for affected organisations. And even if certification of the ISMS is not yet required, there are first signs that this circumstance could change in the medium term - at least for business-critical processes.

Author

Waldemar Grudzien is Expert Director at CORE. He holds a doctorate in electrical engineering and a degree in economics. His work focuses on information security and data protection - in theory and practice, including his work as an ISO and DPO in various client structures.

Mail: waldemar.grudzien@core.se

Moritz Treutwein is Transformation Manager at CORE. His consulting focus is Banking & Capital Markets, and his expertise includes the management and implementation of business area expansions in the context of IT implementation projects, audit remediations, and the development of digital business models. He is also CORE's Information Security Officer.

Mail: moritz.treutwein@core.se

Leon Kuhlmann is Transformation Director at CORE. With his "international business" background and experience in agile and classic project management, he supports clients in the implementation of complex IT transformations. His focus ranges from strategy development to go-live. His current activities include programme initiatives for IT compliance and core banking transformations.

Mail: leon.kuhlmann@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zurich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se